UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

In re Center for Vein Restoration Data Breach Litigation	Master File No.: 1:24-cv-03593 **CONSOLIDATED CLASS ACTION COMPLAINT** **Jury Trial Demanded**

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Aida Khalil, Edward Cameron, Jessica Kayrouz, Katrina Kelley, Lee Conrad, Patricia Knott, Colleen Baird, Gary Scott, Marie E. Wengert, Carla Jackson, and Barbara Voron ("Plaintiffs"), individually and on behalf of all others similarly situated, bring this consolidated class action complaint against Defendant Center for Vein Restoration (MD), LLC ("CVR" or "Defendant") to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of counsel, and the facts that are a matter of public record.

NATURE OF THE ACTION

1. Plaintiffs bring this class action against Defendant for its failure to properly secure and safeguard personally identifiable information ("PII") and protected health information ("PHI") including, but not limited to, particularly sensitive and high-risk information such as dates of birth, Social Security numbers, driver's license numbers, medical record numbers, diagnoses, lab results, medications, treatment information, health insurance information, provider names, dates of treatment, and/or financial information, accompanied by victims' names and addresses.

(collectively, "Private Information").[1]

2. Defendant is (or claims to be) the largest physician-led vein center, which since 2007, has built a medical practice that now includes over 110 locations in 22 states across the United States. Its headquarters are located in Glenn Dale, Maryland.[2]

3. Plaintiffs and Class Members are current or former patients of Defendant.

4. In or before December 2024, Defendant announced on its website that on "October 6, 2024, Center for Vein Restoration was alerted to unusual activity involving our information technology environment."

5. Through the ransomware attack, criminal cyberthieves accessed and exfiltrated Plaintiffs' and Class Members' Private Information.

6. Based upon the investigation, Defendant originally determined that approximately 448,891 victims had their individual Private Information accessed in the Data Breach.[3]

7. Despite first becoming aware of the Data Breach on or around October 6, 2024, and the breach apparently beginning on or before September 30, 2024 (according to Defendant's notice on the Maine AG's website), Defendant did not begin notifying Plaintiffs and other Class Members until on or around December 6, 2024.[4]

---

[1] *Data Breach Notifications*, Office of the Maine Att'y Gen., https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/26220cc6-86d0-41e4-bd2e-60025867aa25.html (last visited Feb. 17, 2025); *see also* Notice of Data Security Incident, attached as Exhibit 1 ("Notice Letter").
[2] https://www.centerforvein.com/find-a-center (last visited Dec. 20, 2024).
[3] *Data Breach Notifications*, Office of the Maine Att'y Gen., https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/26220cc6-86d0-41e4-bd2e-60025867aa25.html (last visited Dec. 20, 2024).
[4] *Id.*

8. As part of its Notice Letter, Defendant disclosed that "[t]he unauthorized party may have accessed files that contain some of your information" including patients' "name in combination with some or all of the following: address, date of birth, Social Security Number, driver's license number, medical record number, diagnosis, lab results, medications, treatment information, health insurance information, provider names, dates of treatment, and/or financial information."[5]

9. As a result of the Data Breach, Plaintiffs and almost 450,000 Class Members suffered injury and ascertainable losses in the form of the present and imminent substantial threat of fraud and identity theft, loss of the benefit of their bargain, out-of-pocket expenses, loss of privacy, loss of value of their time reasonably incurred to remedy or mitigate the effects of the attack, and the loss of, and diminution in, value of their personal information.

10. Plaintiffs' and Class Members' sensitive confidential Private Information was compromised and unlawfully accessed due to the Data Breach. This information, while compromised and taken by unauthorized third parties, also remains in the possession of Defendant, and without additional safeguards and independent review and oversight, remains vulnerable to additional hackers and theft.

11. Particularly alarming is the fact that the Private Information compromised in the Data Breach included Social Security numbers, which are durable and difficult to change.

12. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect Plaintiffs' and Class Members' Private Information.

13. Plaintiffs bring this action on behalf of all persons whose Private Information was

[5] *See* Notice Letter, Ex. 1.

compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure its network containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal statutes.

14. The mechanism of the hacking and potential for improper disclosure of Private Information was a known risk to Defendant and entities like it, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition and vulnerable to theft.

15. Defendant disregarded the rights of Plaintiffs and Class Members by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard patient Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; failing to properly train its staff and employees on proper security measures; and failing to provide Plaintiffs and Class Members prompt notice of the Data Breach.

16. Plaintiffs' and Class Members' identities are now at a substantial and imminent risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves. This present risk will continue for their respective lifetimes.

17. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain

government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

18. Upon information and belief, based on the type of sophisticated and malicious criminal activity, the type of Private Information targeted, Defendant's admission that the Private Information was accessed and exfiltrated, and Defendant's admission that an extensive trove of Plaintiffs and Class Members' Private Information was in the files that were accessed, Plaintiffs and Class Members' Private Information was likely accessed, exfiltrated, stolen, disseminated, and used by a criminal third party.

19. Moreover, as a result of the Data Breach, given the criminal targeting of the Private Information, the sensitive nature of the information, the likelihood of exfiltration, and reports of actual fraud following the Data Breach, Plaintiffs and Class Members are now experiencing a current, imminent, ongoing, and substantial risk of fraud and identity theft. The risk of identity theft is not speculative or hypothetical but is impending and has materialized. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

20. By waiting to notify Plaintiffs and Class Members, Defendant harmed Plaintiffs and Class Members. Put differently, Defendant had a duty to monitor its computer networks, but failed to do so, resulting in the breach going undetected for an undisclosed period of time. Then, if Defendant had notified Plaintiffs and Class Members at or around the time the Data Breach was first discovered in October 2024 instead of waiting two months until December 2024, Plaintiffs and Class Members would have been in a better position to protect themselves and to mitigate their injuries.

21. Despite Defendant offering inadequate credit monitoring services for a period of time, Plaintiffs and Class Members will incur out of pocket costs including but not limited to purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft beyond the inadequate services offered by Defendant.

22. Plaintiffs and Class Members suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) out-of-pocket expenses associated with prevention, detection, and recovery from identity theft, tax fraud and/or unauthorized use of their Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) lost or diminished value of their Private Information; (v) loss of benefit of the bargain; (vi) future costs of ongoing credit and identity theft monitoring; (vii) statutory damages; (viii); nominal damages; (ix) and the ongoing risk of harm as long as Defendant maintains Plaintiffs' and Class Members' Private Information with inadequate security practices.

23. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach.

24. Plaintiffs seek remedies including, but not limited to, compensatory damages, nominal damages, and reimbursement of out-of-pocket costs.

25. Plaintiffs also seeks injunctive and equitable relief to prevent future injury on behalf of themselves and the putative Class.

PARTIES

26. Plaintiff Aida Khalil is and at all times mentioned herein was an individual citizen of the State of Maryland.

27. Plaintiff Edward Cameron is and at all times mentioned herein was an individual

citizen of the State of Maryland.

28. Plaintiff Jessica Kayrouz is and at all times mentioned herein was an individual citizen of the State of Indiana.

29. Plaintiff Katrina Kelley is and at all times mentioned herein was an individual citizen of the State of Illinois.

30. Plaintiff Lee Conrad is and at all times mentioned herein was an individual citizen of the Commonwealth of Virginia.

31. Plaintiff Patricia Knott is and at all times mentioned herein was an individual citizen of the State of New Jersey.

32. Plaintiff Colleen Baird is and at all times mentioned herein was an individual citizen of the State of Maryland.

33. Plaintiff Gary Scott is and at all times mentioned herein was an individual citizen of the State of Georgia.

34. Plaintiff Marie E. Wengert is and at all times mentioned herein was an individual citizen of the State of Maryland.

35. Plaintiff Carla Jackson is and at all times mentioned herein was an individual citizen of the State of Alabama.

36. Plaintiff Barbara Voron is and at all times mentioned herein was an individual citizen of the State of New Jersey.

37. Defendant Center for Vein Restoration (MD), LLC d/b/a Center for Vein Restoration is a Maryland limited liability company that has its principal office at 12200 Annapolis Road, Glenn Dale, Maryland 20769. It can be served through its registered agent at The Corporation Trust, Incorporated, 2405 York Road, Suite 201, Lutherville Timonium, Maryland

21093-2264.

JURISDICTION AND VENUE

38. The Court has subject-matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5,000,000 exclusive of interest and costs; there are more than 100 members in the proposed class; and at least one member of the class, including several named Plaintiffs, is a citizen of a state different from Defendant.[6]

39. The Court has personal jurisdiction over Defendant named in this action because Defendant and/or its parents or affiliates are headquartered in Maryland, and Defendant conducts substantial business in Maryland with at least 15 medical locations in Maryland.

40. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

FACTUAL ALLEGATIONS

41. Defendant is a healthcare provider group that provides a wide range of "vein care" services. Defendant represents to its patients that, since 2007, it has been "the clinical leader in vein care, has offered personalized, cutting-edge vein treatment options in a caring, supportive, office-based environment" and that "[c]hronic venous insufficiency, the root cause of varicose

[6] *See Data Breach Notifications*, Office of the Maine Att'y Gen., https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/26220cc6-86d0-41e4-bd2e-60025867aa25.html, which lists 83 residents of Maine being affected (last visited Feb. 20, 2025); *and Data Breach Report*, Office of the Texas Attorney General, https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage, which lists 31823 residents of Texas being affected (last visited Feb. 20. 2025).

veins and spider veins, affects more than 25 million people in the United States."[7]

42. In its Patient Handbook, Defendant states that it impacts "the lives of over 200,000 patients annually. We conduct more vein procedures than any other vein clinic or hospital. Our practice, the largest of its kind, is built on experience, expertise, and trust. Our team of board-certified physicians and vein care specialists will provide the safest, most positive treatment outcomes."[8]

43. Defendant offers comprehensive vein care and conducts its medical procedures in at least 22 states and the District of Columbia.[9]

44. As part of its medical and business operations, Defendant collects, maintains, and stores the highly sensitive Private Information provided by its current and former patients, including but not limited to: full names, contact information including addresses and telephone numbers, dates of birth, Social Security numbers, employment information, driver's license numbers, medical record numbers, diagnoses, lab results, medications, treatment information, health insurance information, provider names, dates of treatment, and financial information. *See* Exhibit 2 (Defendant's patient intake forms, as provided by Plaintiff Cameron).

45. Defendant also creates and stores medical records and other protected health information for its patients, records of treatments, and diagnoses.

46. Defendant's Patient Privacy and HIPAA Protection Form states: "***Maintaining the privacy of your information is paramount at Center for Vein Restoration (CVR)***." *See* Exhibit 3 (emphasis added). It goes on to assure: "CVR limits the use and disclosure of your PHI to the

[7] https://www.centerforvein.com/ (last visited Dec. 20, 2024).
[8] https://www.centerforvein.com/patient-resources/patient-forms (Patient Handbook, English) (last visited Feb. 20, 2025).
[9] https://www.centerforvein.com/our-clinics/locations (last visited Feb. 20. 2025).

minimum amount necessary. When release of PHI is required, our staff will seek your written authorization prior to release and maintain a record of all PHI disclosures." *Id.* Defendant provided this Patient Privacy and HIPAA Protection Form to Plaintiff Cameron.

47. In addition, upon information and belief, Defendant's Privacy Policy (the "Privacy Policy") was provided to every patient both prior to receiving treatment and upon request. Defendant's Privacy Policy makes clear that it understands that its patients' Private Information is personal and must be protected by law.[10] *See* Exhibit 3 ("*A copy of the Notice can be provided for your review at registration and can be accessed at the CVR website*."). Defendant "provides services to a number of health care providers that are subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA). When [Defendant] collects, uses, and discloses personal information for or on behalf of these health care providers, [it] does so in its capacity as a 'business associate' to those health care providers. Such personal information is subject to [it]s agreements with its health care providers and their Notice of Privacy Practices, https://www.centerforvein.com/assets/documents/CVR-Notice-of-Privacy-Practices.pdf."[11]

48. Defendant agreed to and did undertake legal duties to maintain the protected health and personal information entrusted to it by Plaintiffs and Class Members safely, confidentially, and in compliance with all applicable laws, including the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, and the Health Insurance Portability and Accountability Act ("HIPAA").

49. Plaintiffs and Class Members, as current and former patients of Defendant, entrusted their Private Information to Defendant with the reasonable expectation that Defendant

[10] https://www.centerforvein.com/privacy-policy (last visited Feb. 20, 2025).
[11] *Id.*

would comply with its obligation to keep their sensitive and personal information confidential and secure from illegal and unauthorized access, and that Defendant would provide them with prompt and accurate notice of any unauthorized access to their Private Information.

50. Unfortunately for Plaintiffs and Class Members, Defendant failed to carry out its duty to safeguard sensitive Private Information and provide adequate data security, thus failing to protect Plaintiffs and Class Members from the exfiltration of their Private Information during the Data Breach.

THE CYBERATTACK AND DATA BREACH

51. According to Defendant's Notice of Data Security Incident (attached in full as Ex. 1) ("Notice Letter"):

> **What Happened?**
> On October 6, 2024, Center for Vein Restoration was alerted to unusual activity involving our information technology environment. In response, we initiated an investigation, took steps to secure our systems, and notified law enforcement. Additionally, a third-party forensic firm was engaged to assist in the investigation.
>
> **What Information Was Involved?**
>
> While in our IT environment, the unauthorized party may have accessed files that contain some of your information, including your name in combination with some or all of the following: address, date of birth, Social Security number, driver's license number, medical record number, diagnosis, lab results, medications, treatment information, health insurance information, provider names, dates of treatment, and/or financial information. For employees, information related to employment may have been impacted.

52. Further, Defendant specifically recommended that Plaintiffs and Class Members monitor "financial statements you receive from your healthcare providers and health insurance plans. If you see any services that were not received, please contact the provider or health plan immediately. Additional information about protecting your identity is included in this letter, including recommendations by the Federal Trade Commission regarding identity theft protection

and details on how to place a fraud alert or a security freeze on your credit file." *See* Ex. 1.

53. Defendant's notice to the Maine Attorney General included additional information, stating that the Data Breach occurred on September 30, 2024, and was not discovered until October 6, 2024. It also reported that the cyberthieves had accessed 448,891 Class Members' Private Information.[12]

54. Defendant failed to notify these individuals identified as affected by the Data Breach until December 12, 2024.[13]

55. Plaintiffs and Class Members have never been fully informed about the scope of the intrusion, the vulnerabilities that were exploited, the remediation that is required, or the lingering vulnerability of their data remaining in Defendant's possession.

56. Through this targeted cyberattack, Plaintiffs' and Class Members' Private Information, including Social Security numbers and PHI, was accessed by cybercriminals.

57. Defendant negligently failed to use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiffs and Class Members, causing the exposure of Private Information for Plaintiffs and Class Members.

58. For example, as evidenced by the Data Breach's occurrence, the infiltrated network was not protected by sufficient multi-layer data security technologies or effective firewalls.

59. Similarly, based on the delayed discovery of the Data Breach, it is evident that the infiltrated network that Defendant allowed to store Plaintiffs' Private Information did not have sufficiently effective endpoint detection.

---

[12] *Data Breach Notifications*, Office of the Maine Att'y Gen., https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/26220cc6-86d0-41e4-bd2e-60025867aa25.html (last visited Feb. 20, 2025).
[13] *Id.*

60. Further, the fact that Private Information was accessible and/or accessed in the Data Breach demonstrates that the Private Information contained in Defendant's network was not encrypted. Had the information been properly encrypted, the data thieves would have only had access to indecipherable data.

61. If Defendant had properly monitored its cyber security systems, it would have prevented the Data Breach, discovered the Data Breach sooner, and/or have prevented the hackers from accessing Plaintiffs' and Class Members' Private Information.

62. The targeted attack was intended to, and did, gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of persons such as Plaintiffs and Class Members.

63. Due to Defendant's inadequate security measures, Plaintiffs and Class Members now face a substantial, present, imminent, and ongoing risk of fraud and identity theft, and must deal with that threat forever.

64. Due to Defendant's inadequate security measures, Plaintiffs' and Class Members' Private Information is now in the hands of cyberthieves.

65. Defendant failed to comply with its obligations to keep such information confidential and secure from unauthorized access, as well as its obligation to timely notify Plaintiffs and Class Members.

THE DATA BREACH WAS FORESEEABLE

66. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches targeting corporations, preceding the date of the breach.

67. Defendant knew and understood that unprotected Private Information is valuable

and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

68. As a custodian of Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiffs and Class Members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiffs and Class Members as a result of a breach.

69. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so that they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store PII are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[14]

70. Therefore, the increase in such attacks, and the attendant risk of future attacks in light of the nature of Defendant's business, was surely known to Defendant. Anyone in Defendant's industry knew or should have known of the risks of a cyberattack and taken sufficient steps to fulfill its obligation to the people who entrust their personal data to the business. Defendant failed to do so.

71. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients,

[14] https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last visited Feb. 20, 2025).

September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

DEFENDANT FAILED TO PROPERLY PROTECT PLAINTIFFS' AND CLASS MEMBERS' PRIVATE INFORMATION

72. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted Private Information it was maintaining for Plaintiffs and Class Members, causing the exposure of Private Information for almost 450,000 individuals.

73. The FTC promulgated numerous guides which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

74. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[15] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[16]

[15] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.
[16] *Id.*

75. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

76. Defendant failed to properly implement basic data security practices explained and set forth by the FTC.

77. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

78. A Data Breach such as the one Defendant experienced, is also considered a breach under the HIPAA Rules because there is an unauthorized access to PHI that is not permitted under HIPAA.

79. A breach under the HIPAA Rules is defined as, "the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." 45 C.F.R. 164.40.

80. Data breaches are also Security Incidents under HIPAA because they impair both the integrity (data is not interpretable) and availability (data is not accessible) of patient health information:

> The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. See the definition of security incident at 45 C.F.R. 164.304. Once the ransomware is detected, the covered entity or business associate must initiate its security incident

and response and reporting procedures. 45 C.F.R.164.308(a)(6).[17]

81. Defendant's Data Breach was the foreseeable consequence of a combination of insufficiencies that demonstrate that Defendant failed to comply with safeguards mandated by HIPAA.

DEFENDANT FAILED TO COMPLY WITH INDUSTRY STANDARDS

82. Defendant did not utilize industry standards appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiffs and Class Members, causing the exposure of Private Information for approximately 448,891 individuals.

83. As explained by the FBI, "[p]revention is the most effective defense against cyberattacks] and it is critical to take precautions for protection."[18]

84. To prevent and detect cyberattacks, including the cyberattack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of cyberattacks and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a

[17] *FACT SHEET: Ransomware and HIPPA*, U.S. Dept. of Health and Hum. Servs., at 4 (July 11, 2016), https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf.
[18] *See* How to Protect Your Networks from RANSOMWARE, at 3, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Dec. 20, 2024).

centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common cyberware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[19]

85. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….
- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you

[19] *Id.* at 3-4.

know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the Internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net) . . .

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[20]

86. To prevent and detect cyberattacks, including the cyberattack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure Internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

[20] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), https://www.cisa.gov/news-events/news/protecting-against-ransomware (last visited Feb. 20, 2025).

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[21]

87. As described above, experts studying cyber security routinely identify medical facilities as being particularly vulnerable to cyberattacks because of the value of the Private Information they collect and maintain.

88. Several best practices have been identified that at a minimum should be implemented by institutions such as Defendant, including, but not limited to, the following: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus,

[21] *See Human-Operated Ransomware Attacks: A Preventable Disaster* (Mar 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

89. Other best cybersecurity practices that are standard include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

90. Defendant failed to meet the minimum standards of any of the following frameworks: NIST Cybersecurity Framework Version 2.0 (including PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

91. Given that Defendant was storing the Private Information of nearly 450,000 individuals, Defendant could and should have implemented all of the above measures to prevent cyberattacks.

92. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of approximately 448,891 individuals' Private Information.

DEFENDANT FAILED TO PROPERLY PROTECT PRIVATE INFORMATION

93. Defendant breached its obligations to Plaintiffs and Class Members and was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts

and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches, cyber-attacks, hacking incidents, and ransomware attacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor its own data security systems for existing or prior intrusions;

d. Failing to test and assess the adequacy of its data security system;

e. Failing to develop adequate training programs related to the proper handling of emails and email security practices;

f. Failing to adequately fund and allocate resources for the adequate design, operation, maintenance, and updating necessary to meet industry standards for data security protection;

g. Failing to require a data security system to ensure the confidentiality and integrity of electronic PHI its network created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

h. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access to only those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

i. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

j. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

k. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

l. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

m. Failing to ensure that it was compliant with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

n. Failing to train all members of its workforce effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI, in violation

of 45 C.F.R. § 164.530(b);

o. Failing to ensure that the electronic PHI it maintained is unusable, unreadable, or indecipherable to unauthorized individuals, as Defendants had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 C.F.R. § 164.304 definition of encryption);

p. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act, and;

q. Failing to adhere to industry standards for cybersecurity.

94. As the result of computer systems in need of security upgrades, inadequate procedures for handling email phishing attacks, viruses, malignant computer code, hacking attacks, Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information.

95. Accordingly, as outlined below, Plaintiffs and Class Members now face a present, increased, and immediate risk of fraud and identity theft.

DATA BREACHES DISRUPT LIVES AND INCREASE RISK OF FRAUD AND IDENTITY THEFT

96. The United States Government Accountability Office has long recognized the costs of a data breach, releasing an extensive report as early as 2007 regarding data breaches ("GAO Report") noting that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[22]

97. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity

[22] *See* U.S. Gov. Accountability Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), https://www.gao.gov/new.items/d07737.pdf.

thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Here, the cyberthieves already have numerous pieces of the Class Members' Private Information, including their Social Security numbers.

98. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[23]

99. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

100. Social Security numbers are among the most dangerous kinds of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number

[23] *See IdentityTheft.gov*, Fed. Trade Comm'n, https://www.identitytheft.gov/Steps (last visited Dec. 20, 2024).

and assuming your identity can cause a lot of problems.[24]

101. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

102. Furthermore, trying to change or cancel a stolen Social Security number is no minor task. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

103. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[25]

104. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than

[24] *Identity Theft and Your Social Security Number*, Social Security Admin. (July 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf.
[25] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

10x on the black market."[26]

105. Moreover, theft of Private Information is also gravely serious. One's Private Information is an extremely valuable asset.[27]

106. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

107. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

108. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

109. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiffs and Class Members must vigilantly monitor their financial information for many years to come.

---

[26] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, COMPUTER WORLD (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[27] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

110. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[28] Private Information is particularly valuable because criminals can use it to target victims with frauds and scams; once stolen, fraudulent use of that information and damage to victims may continue for years.

111. Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that victims were often forced to pay out of pocket costs for healthcare they did not receive in order to restore coverage.[29] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. 40 percent of the patients were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals, and detrimentally impact the economy as a whole.[30]

112. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

113. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain and piece together information about that person's identity, such as login credentials or Social Security numbers. Social engineering is a form of hacking whereby a data thief uses previously acquired information to

---

[28] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.
[29] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/.
[30] *See id.*

manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches can be the starting point for these additional targeted attacks on the victim.

114. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[31]

115. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. Even if certain information (such as emails, phone numbers, or credit card numbers) are not included in the Private Information that was exfiltrated from this Data Breach, criminals may still easily create a Fullz package to sell at a higher price to unscrupulous operators and criminals.

PLAINTIFFS' EXPERIENCES

Plaintiff Aida Khalil

116. Plaintiff Khalil provided her Private Information to Defendant to obtain health care services from Defendant.

117. At the time of the Data Breach, Defendant retained Plaintiff Khalil's Private Information in its system.

[31] "Fullz" is a term used to describe the practice of collecting, then selling, the information of a data breach victim from multiple sources, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information criminals have on a victim, the more money that can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. *See, e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm*, Krebs on Security (Sept. 18, 2014), https://krebsonsecuritv.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas- life-insurance-firm.

118. Plaintiff Khalil received a Notice Letter from Defendant dated December 12, 2024, informing her that her Private Information—including her Social Security number and medical treatment information—was specifically identified as having been exposed to cybercriminals in the Data Breach.

119. Plaintiff Khalil takes reasonable measures to protect her Private Information. She has never knowingly transmitted unencrypted Private Information over the Internet or other unsecured source.

120. Plaintiff Khalil stores any documents containing her Private Information in a safe and secure location and diligently chooses unique usernames and passwords for her online accounts.

121. Because of the Data Breach, Plaintiff Khalil's Private Information is now in the hands of cybercriminals.

122. Plaintiff Khalil has been injured by the compromise of her Private Information. As a result of the Data Breach, which exposed highly valuable information such as her Social Security number, she is now imminently at risk of crippling future identity theft and fraud for her lifetime.

123. Since the Data Breach, Plaintiff Khalil has already experienced data misuse. For example, after the Data Breach, Plaintiff Khalil experienced unauthorized transactions on her financial account. Furthermore, in October 2024, Plaintiff Khalil noticed unauthorized credit inquiries on her credit report, which caused her credit score to drop. Additionally, Plaintiff Khalil has experienced a notable increase in spam calls and texts following the Data Breach. Plaintiff Khalil attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity and the fact that she has never experienced anything like this prior to now.

124. Further, as a result of the Data Breach, Plaintiff Khalil has had no choice but to

spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Khalil has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing account statements and other information, monitoring her credit reports on a regular basis, reviewing her credit monitoring notifications, and taking other protective and ameliorative steps in response to the Data Breach. This is time that was lost and unproductive and took away from other activities and work duties.

125. The letter Plaintiff Khalil received from Defendant specifically directed her to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised them to "remain vigilant by reviewing account statements and monitoring credit reports."[32] In addition, the breach notification letter listed several "recommended steps" that victims of the Data Breach should take to help protect themselves including enrolling in credit monitoring, monitoring accounts, reviewing credit reports, placing fraud alerts with credit reporting bureaus, and placing security freezes on credit reports.[33]

126. As a result of the Data Breach, Plaintiff Khalil has experienced stress, anxiety, fear and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing and misusing her Private Information. In particular, Plaintiff Khalil is concerned that fraudulent transactions and the unauthorized credit inquiries may harm her credit or her personal finances.

127. Plaintiff Khalil has anxiety and increased concerns for the loss of her privacy. She

[32] *See* Breach Notice Letter (Exhibit 1), available at: https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/26220cc6-86d0-41e4-bd2e-60025867aa25.html.
[33] *Id.*

has spent and anticipates continuing to spend considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

128. Plaintiff Khalil has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Khalil's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Khalil's Private Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Khalil's Private Information; and (e) continued risk to Plaintiff Khalil's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

Plaintiff Edward Cameron

129. In exchange for medical services, Plaintiff Cameron entrusted his Private Information to Defendant. Pursuant to HIPAA, Defendant was required to protect and maintain the confidentiality of Private Information entrusted to it.

130. Plaintiff Cameron received a Notice Letter from Defendant dated December 12, 2024, informing him that his Private Information—including his Social Security number, and medical treatment information—was specifically identified as having been exposed to cybercriminals in the Data Breach.

131. Plaintiff Cameron is very careful about sharing his sensitive information.

132. Plaintiff Cameron stores any documents containing his Private Information in a safe

and secure location. Plaintiff Cameron has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

133. Because of the Data Breach, Plaintiff Cameron's Private Information is now in the hands of cybercriminals.

134. Plaintiff Cameron has suffered actual injury from the exposure and theft of his Private Information—which violates his right to privacy.

135. As a result of the Data Breach, which exposed highly valuable information such as his Social Security number, Plaintiff Cameron is now imminently at risk of crippling future identity theft and fraud for his lifetime.

136. Since the Data Breach, Plaintiff Cameron has already experienced data misuse. For example, in the months following the Data Breach, Plaintiff Cameron has received notifications that his Private Information has been located on the dark web. Additionally, Plaintiff Cameron has experienced a notable increase in spam calls and texts following the Data Breach. Some of these recent spam calls and texts relate to medical care, pharmaceuticals, or other age-related solicitations. Plaintiff Cameron attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity and the fact that these occurrences are highly unusual.

137. Further, as a result of the Data Breach, Plaintiff Cameron has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Cameron has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate and mitigate the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing account statements and other information, screening and addressing spam correspondence, reviewing his credit monitoring reports and notifications,

and taking other protective and ameliorative steps in response to the Data Breach. This is time that was lost and unproductive and took away from other activities, including work, recreation, and family duties.

138. The letter Plaintiff Cameron received from Defendant specifically directed him to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised them to "remain vigilant by reviewing account statements and monitoring credit reports."[34] In addition, the breach notification letter listed several "recommended steps" that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, reviewing credit reports, placing fraud alerts with credit reporting bureaus, and placing security freezes on credit reports.[35]

139. As a result of the Data Breach, Plaintiff Cameron has experienced stress, anxiety, fear and concern due to the loss of his privacy and concern over the impact of cybercriminals accessing and misusing his Private Information. Plaintiff Cameron fears that criminals will use his information to commit identity theft, which could result in financial damage to him.

140. Plaintiff Cameron has spent and anticipates continuing to spend considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

141. Plaintiff Cameron has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Cameron's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Cameron's Private Information that was entrusted to Defendant; (d) damages

[34] *Id.*
[35] *Id.*

unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Cameron's Private Information; and (e) continued risk to Plaintiff Cameron's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

Plaintiff Jessica Kayrouz

142. Plaintiff Kayrouz entrusted her sensitive Private Information to Defendant in exchange for medical services.

143. Plaintiff Kayrouz received a Notice Letter from Defendant dated December 12, 2024, informing her that her Private Information—including her Social Security number, and medical treatment information—was specifically identified as having been exposed to cybercriminals in the Data Breach.

144. Plaintiff Kayrouz is very careful about sharing her sensitive information.

145. Plaintiff Kayrouz stores any documents containing her Private Information in a safe and secure location. Plaintiff Kayrouz has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

146. Because of the Data Breach, Plaintiff Kayrouz's Private Information is now in the hands of cybercriminals.

147. Plaintiff Kayrouz has suffered actual injury from the exposure and theft of her Private Information—which violates her right to privacy.

148. As a result of the Data Breach, which exposed highly valuable information such as her Social Security number, Plaintiff Kayrouz is now imminently at risk of crippling future identity

theft and fraud for her lifetime.

149. Since the Data Breach, Plaintiff Kayrouz has already experienced data misuse. Specifically, after the Data Breach, Plaintiff Kayrouz has received notifications that her Private Information has been located on the dark web. Furthermore, Plaintiff Kayrouz has experienced a notable increase in spam calls, texts, and emails following the Data Breach. Plaintiff Kayrouz attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity and the fact that she has never experienced anything like this prior to now.

150. Further, as a result of the Data Breach, Plaintiff Kayrouz has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Kayrouz has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate and mitigate the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing account statements and account activity, reviewing her credit monitoring alerts and dark web notifications, and taking other protective and ameliorative steps in response to the Data Breach. This is time that was lost and unproductive and took away from other activities and work duties.

151. The letter Plaintiff Kayrouz received from Defendant specifically directed her to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised them to "remain vigilant by reviewing account statements and monitoring credit reports."[36] In addition, the breach notification letter listed several "recommended steps" that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, reviewing credit reports, placing fraud alerts with credit

[36] *Id.*

reporting bureaus, and placing security freezes on credit reports.[37]

152. As a result of the Data Breach, Plaintiff Kayrouz has experienced stress, anxiety, fear and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing and misusing her Private Information. In particular, Plaintiff Kayrouz is concerned that identity fraud she has experienced or may experience in the future will harm her credit or her personal finances.

153. Plaintiff Kayrouz has spent and anticipates continuing to spend considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

154. Plaintiff Kayrouz has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Kayrouz's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Kayrouz's Private Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Kayrouz's Private Information; and (e) continued risk to Plaintiff Kayrouz's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

Plaintiff Katrina Kelley

155. Plaintiff Kelley entrusted her sensitive Private Information to Defendant in

[37] *Id.*

exchange for medical services.

156. Plaintiff Kelley received a Notice Letter from Defendant dated December 12, 2024, informing her that her Private Information—including her Social Security number, and medical treatment information—was specifically identified as having been exposed to cybercriminals in the Data Breach.

157. Plaintiff Kelley is very careful about sharing her sensitive information.

158. Plaintiff Kelley stores any documents containing her Private Information in a safe and secure location. Plaintiff Kelley has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

159. Because of the Data Breach, Plaintiff Kelley's Private Information is now in the hands of cybercriminals.

160. Plaintiff Kelley has suffered actual injury from the exposure and theft of her Private Information—which violates her right to privacy.

161. As a result of the Data Breach, which exposed highly valuable information such as her Social Security number, Plaintiff Kelley is now imminently at risk of crippling future identity theft and fraud for her lifetime.

162. Since the Data Breach, Plaintiff Kelley has already experienced identity fraud. For example, after the Data Breach, Plaintiff Kelley experienced fraudulent transactions on her Discover card wherein someone made multiple unauthorized purchases. Plaintiff Kelley has also received notifications that her Private Information has been located on the dark web since the Data Breach. Furthermore, Plaintiff Kelley has experienced a notable increase in spam calls, texts, and emails following the Data Breach, including emails with fraudulent invoices. Plaintiff Kelley attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time

proximity and the fact that she has never experienced anything like this prior to now.

163. Further, as a result of the Data Breach, Plaintiff Kelley has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Kelley has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, and mitigate the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing account statements and account activity on a daily basis, contacting her bank, reviewing her identity theft and credit monitoring notifications, and taking other protective and ameliorative steps in response to the Data Breach. This is time that was lost and unproductive and took away from other activities, work, and family duties.

164. The letter Plaintiff Kelley received from Defendant specifically directed her to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised them to "remain vigilant by reviewing account statements and monitoring credit reports."[38] In addition, the breach notification letter listed several "recommended steps" that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, reviewing credit reports, placing fraud alerts with credit reporting bureaus, and placing security freezes on credit reports.[39]

165. As a result of the Data Breach, Plaintiff Kelley has experienced stress, anxiety, fear and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing and misusing her Private Information. In particular, Plaintiff Kelley is concerned that identity fraud she has experienced or may experience in the future will harm her credit or her personal finances.

[38] *Id.*
[39] *Id.*

166. Plaintiff Kelley has spent and anticipates continuing to spend considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

167. Plaintiff Kelley has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Kelley's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Kelley's Private Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Kelley's Private Information; and (e) continued risk to Plaintiff Kelley's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

Plaintiff Lee Conrad

168. Plaintiff Conrad entrusted his sensitive Private Information to Defendant in exchange for medical services.

169. Plaintiff Conrad received a Notice Letter from Defendant dated December 12, 2024, informing him that his Private Information—including his Social Security number, and medical treatment information—was specifically identified as having been exposed to cybercriminals in the Data Breach.

170. Plaintiff Conrad is very careful about sharing his sensitive information.

171. Plaintiff Conrad stores any documents containing his Private Information in a safe

and secure location. Plaintiff Conrad has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

172. Because of the Data Breach, Plaintiff Conrad's Private Information is now in the hands of cybercriminals.

173. Plaintiff Conrad has suffered actual injury from the exposure and theft of his Private Information—which violates his right to privacy.

174. As a result of the Data Breach, which exposed highly valuable information such as his Social Security number, Plaintiff Conrad is now imminently at risk of crippling future identity theft and fraud for his lifetime.

175. Since the Data Breach, Plaintiff Conrad has already experienced identity theft and fraud. For example, in December 2024, he was notified by his bank that five unauthorized charges were made to his account, collectively totaling approximately $5000. Since the Data Breach, Plaintiff Conrad was also separately notified of fraudulent attempts to apply for credit cards using his Private Information. Additionally, Plaintiff Conrad has experienced a notable increase in spam calls and texts, including scams, following the Data Breach. Plaintiff Conrad attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity and the fact that he has never before experienced anything like this.

176. Further, as a result of the Data Breach, Plaintiff Conrad has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Conrad has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate and mitigate the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing account statements and other information, screening and addressing

spam correspondence, reviewing his credit monitoring reports and notifications, and taking other protective and ameliorative steps in response to the Data Breach. Trying to get the fraudulent charges reversed has caused all sorts of banking problems and has taken hours of his personal time, including going to the bank, which he could have and would have used in more productive ways.

177. The letter Plaintiff Conrad received from Defendant specifically directed him to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised them to "remain vigilant by reviewing account statements and monitoring credit reports."[40] In addition, the breach notification letter listed several "recommended steps" that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, reviewing credit reports, placing fraud alerts with credit reporting bureaus, and placing security freezes on credit reports.[41]

178. As a result of the Data Breach, Plaintiff Conrad has experienced stress, anxiety, fear and concern due to the loss of his privacy and concern over the impact of cybercriminals accessing and misusing his Private Information. Plaintiff Conrad now constantly worries that criminals will use his information to commit identity theft, which could result in financial damage to him.

179. Plaintiff Conrad has spent and anticipates continuing to spend considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

180. Plaintiff Conrad has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Conrad's

[40] *Id.*
[41] *Id.*

Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Conrad's Private Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Conrad's Private Information; and (e) continued risk to Plaintiff Conrad's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

Plaintiff Patricia Knott

181. Plaintiff Knott entrusted her sensitive Private Information to Defendant in exchange for medical services.

182. Plaintiff Knott received a Notice Letter from Defendant dated December 12, 2024, informing her that her Private Information was specifically identified as having been exposed to cybercriminals in the Data Breach.

183. Plaintiff Knott is very careful about sharing her sensitive information.

184. Plaintiff Knott stores any documents containing her Private Information in a safe and secure location. Plaintiff Knott has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

185. Because of the Data Breach, Plaintiff Knott's Private Information is now in the hands of cybercriminals.

186. Plaintiff Knott has suffered actual injury from the exposure and theft of her Private Information—which violates her right to privacy.

187. As a result of the Data Breach, which exposed highly valuable information such as her Social Security number, Plaintiff Knott is now imminently at risk of crippling future identity theft and fraud for her lifetime.

188. Further, as a result of the Data Breach, Plaintiff Knott has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Knott has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate and mitigate the future consequences of the Data Breach, including monitoring her credit information, changing passwords on her various accounts, and taking other protective and ameliorative steps in response to the Data Breach. This is time that was lost and unproductive and took away from other activities, work, and family time.

189. The letter Plaintiff Knott received from Defendant specifically directed her to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised them to "remain vigilant by reviewing account statements and monitoring credit reports."[42] In addition, the breach notification letter listed several "recommended steps" that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, reviewing credit reports, placing fraud alerts with credit reporting bureaus, and placing security freezes on credit reports.[43]

190. As a result of the Data Breach, Plaintiff Knott has experienced stress, anxiety, fear and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing and misusing her Private Information. Plaintiff Knott fears that criminals will use her information

[42] *Id.*
[43] *Id.*

to commit identity theft.

191. Plaintiff Knott has spent and anticipates continuing to spend considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

192. Plaintiff Knott has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Knott's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Knott's Private Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Knott's Private Information; and (e) continued risk to Plaintiff Knott's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant

Plaintiff Colleen Baird

193. Plaintiff Baird entrusted her sensitive Private Information to Defendant in exchange for medical services.

194. Plaintiff Baird received a Notice Letter from Defendant dated December 12, 2024, informing her that her Private Information—including her Social Security number, and medical treatment information—was specifically identified as having been exposed to cybercriminals in the Data Breach.

195. Plaintiff Baird is very careful about sharing her sensitive information.

196. Plaintiff Baird stores any documents containing her Private Information in a safe and secure location. Plaintiff Baird has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

197. Because of the Data Breach, Plaintiff Baird's Private Information is now in the hands of cybercriminals.

198. Plaintiff Baird has suffered actual injury from the exposure and theft of her Private Information—which violates her right to privacy.

199. As a result of the Data Breach, which exposed highly valuable information such as her Social Security number, Plaintiff Baird is now imminently at risk of crippling future identity theft and fraud for her lifetime.

200. Since the Data Breach, Plaintiff Baird has already experienced data misuse. For example, in the months following the Data Breach, Plaintiff Baird has received notifications that her Private Information has been located on the dark web. Additionally, Plaintiff Baird has experienced a notable increase in spam calls and texts following the Data Breach. Plaintiff Baird attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity and the fact that, to her knowledge, her Private Information has never before been posted on the dark web.

201. As a result of the Data Breach and the subsequent notifications advising her that her Private Information has been placed on the dark web, Plaintiff Baird has expended her own money to purchase identity theft protection services through LifeLock at a cost of $95.39 per year.

202. Further, as a result of the Data Breach, Plaintiff Baird has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Baird has already expended

time and suffered loss of productivity from taking time to address and attempt to ameliorate and mitigate the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing account statements and other information, placing credit freezes with all three credit bureaus, researching and purchasing identity theft protection services, reviewing her credit monitoring reports and notifications, and taking other protective and ameliorative steps in response to the Data Breach. This is time that was lost and unproductive and took away from other activities, work, and family time.

203. The letter Plaintiff Baird received from Defendant specifically directed her to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised them to "remain vigilant by reviewing account statements and monitoring credit reports."[44] In addition, the breach notification letter listed several "recommended steps" that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, reviewing credit reports, placing fraud alerts with credit reporting bureaus, and placing security freezes on credit reports.[45]

204. As a result of the Data Breach, Plaintiff Baird has experienced stress, anxiety, fear and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing and misusing her Private Information. Plaintiff Baird fears that criminals will use her information to commit identity theft.

205. Plaintiff Baird has spent and anticipates continuing to spend considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

206. Plaintiff Baird has also suffered injury directly and proximately caused by the Data

[44] *Id.*
[45] *Id.*

Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Baird's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Baird's Private Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Baird's Private Information; and (e) continued risk to Plaintiff Baird's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

Plaintiff Gary Scott

207. Plaintiff Gary Scott is a former patient of Defendant.

208. Plaintiff Scott entrusted his sensitive Private Information to Defendant in exchange for medical services.

209. Plaintiff Scott received a Notice Letter from Defendant dated December 12, 2024, informing him that his Private Information—including his Social Security number, and medical treatment information—was specifically identified as having been exposed to cybercriminals in the Data Breach.

210. Plaintiff Scott is very careful about sharing his sensitive information.

211. Plaintiff Scott stores any documents containing his Private Information in a safe and secure location. Plaintiff Scott has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

212. Because of the Data Breach, Plaintiff Scott's Private Information is now in the

hands of cybercriminals.

213. Plaintiff Scott has suffered actual injury from the exposure and theft of his Private Information—which violates his right to privacy.

214. As a result of the Data Breach, which exposed highly valuable information such as his Social Security number, Plaintiff Scott is now imminently at risk of crippling future identity theft and fraud for his lifetime.

215. Since the Data Breach, Plaintiff Scott has experienced a notable increase in suspicious calls and texts.

216. As a result of the Data Breach, Plaintiff Scott has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Scott has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate and mitigate the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing account statements and other information, and taking other protective and ameliorative steps in response to the Data Breach. This is time he could have and would have used in more productive ways, including work or leisure time.

217. The letter Plaintiff Scott received from Defendant specifically directed him to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised them to "remain vigilant by reviewing account statements and monitoring credit reports."[46] In addition, the breach notification letter listed several "recommended steps" that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, reviewing credit reports, placing fraud alerts with credit

[46] *Id.*

reporting bureaus, and placing security freezes on credit reports.[47]

218. As a result of the Data Breach, Plaintiff Scott has experienced stress, anxiety, fear and concern due to the loss of his privacy and concern over the impact of cybercriminals accessing and misusing his Private Information. Plaintiff Scott now constantly worries that criminals will use his information to commit identity theft, which could result in financial damage to him.

219. Plaintiff Scott has spent and anticipates continuing to spend considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

220. Plaintiff Scott has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Scott's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Scott's Private Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Scott's Private Information; and (e) continued risk to Plaintiff Scott's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant

Plaintiff Marie E. Wengert

221. Plaintiff Wengert is a former patient of Defendant, having received services from Defendant in 2019.

[47] *Id.*

222. Plaintiff Wengert entrusted her sensitive Private Information to Defendant in exchange for medical services.

223. Plaintiff Wengert received a Notice Letter from Defendant dated December 12, 2024, informing her that her Private Information—including her Social Security number, and medical treatment information—was specifically identified as having been exposed to cybercriminals in the Data Breach.

224. Plaintiff Wengert is very careful about sharing her sensitive information.

225. Plaintiff Wengert stores any documents containing her Private Information in a safe and secure location. Plaintiff Wengert has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

226. Because of the Data Breach, Plaintiff Wengert's Private Information is now in the hands of cybercriminals.

227. Plaintiff Wengert has suffered actual injury from the exposure and theft of her Private Information—which violates her right to privacy.

228. As a result of the Data Breach, which exposed highly valuable information such as her Social Security number, Plaintiff Wengert is now imminently at risk of crippling future identity theft and fraud for her lifetime.

229. Since the Data Breach, Plaintiff Wengert has experienced a notable increase in suspicious calls and texts.

230. Further, as a result of the Data Breach, Plaintiff Wengert has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Wengert has already expended time and suffered loss of productivity from taking time to address and attempt to

ameliorate and mitigate the future consequences of the Data Breach, including researching facts about the Data Breach, reviewing account statements and other information, monitoring her transactions and account activity on a regular basis, and taking other protective and ameliorative steps in response to the Data Breach. This is time that was lost and unproductive and took away from other activities, work, and family time.

231. The letter Plaintiff Wengert received from Defendant specifically directed her to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised them to "remain vigilant by reviewing account statements and monitoring credit reports."[48] In addition, the breach notification letter listed several "recommended steps" that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, reviewing credit reports, placing fraud alerts with credit reporting bureaus, and placing security freezes on credit reports.[49]

232. As a result of the Data Breach, Plaintiff Wengert has experienced stress, anxiety, fear and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing and misusing her Private Information. Plaintiff Wengert fears that criminals will use her information to commit identity theft.

233. Plaintiff Wengert has spent and anticipates continuing to spend considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

234. Plaintiff Wengert has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Wengert's

[48] *Id.*
[49] *Id.*

Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Wengert's Private Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Wengert's Private Information; and (e) continued risk to Plaintiff Wengert's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

Plaintiff Carla Jackson

235. Plaintiff Jackson entrusted her sensitive Private Information to Defendant in exchange for medical services.

236. Plaintiff Jackson received a Notice Letter from Defendant dated December 12, 2024, informing her that her Private Information—including her Social Security number, and medical treatment information—was specifically identified as having been exposed to cybercriminals in the Data Breach.

237. Plaintiff Jackson is very careful about sharing her sensitive information.

238. Plaintiff Jackson stores any documents containing her Private Information in a safe and secure location. Plaintiff Jackson has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

239. Because of the Data Breach, Plaintiff Jackson's Private Information is now in the hands of cybercriminals.

240. Plaintiff Jackson has suffered actual injury from the exposure and theft of her Private Information—which violates her right to privacy.

241. As a result of the Data Breach, which exposed highly valuable information such as her Social Security number, Plaintiff Jackson is now imminently at risk of crippling future identity theft and fraud for her lifetime.

242. Further, as a result of the Data Breach, Plaintiff Jackson has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Jackson has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate and mitigate the future consequences of the Data Breach, including researching facts about the Data Breach, reviewing account statements and other information, monitoring her transactions and account activity on a regular basis, and taking other protective and ameliorative steps in response to the Data Breach. This is time that was lost and unproductive and took away from other activities, work, and family time.

243. The letter Plaintiff Jackson received from Defendant specifically directed her to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised them to "remain vigilant by reviewing account statements and monitoring credit reports."[50] In addition, the breach notification letter listed several "recommended steps" that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, reviewing credit reports, placing fraud alerts with credit reporting bureaus, and placing security freezes on credit reports.[51]

244. As a result of the Data Breach, Plaintiff Jackson has experienced stress, anxiety, fear and concern due to the loss of her privacy and concern over the impact of cybercriminals

[50] *Id.*
[51] *Id.*

accessing and misusing her Private Information. Plaintiff Jackson fears that criminals will use her information to commit identity theft.

245. Plaintiff Jackson has spent and anticipates continuing to spend considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

246. Plaintiff Jackson has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Jackson's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Jackson's Private Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Jackson's Private Information; and (e) continued risk to Plaintiff Jackson's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

Plaintiff Barbara Voron

247. Plaintiff Voron entrusted her sensitive Private Information to Defendant in exchange for medical services.

248. Plaintiff Voron received a Notice Letter from Defendant dated December 12, 2024, informing her that her Private Information—including her Social Security number, and medical treatment information—was specifically identified as having been exposed to cybercriminals in the Data Breach.

249. Plaintiff Voron is very careful about sharing her sensitive information.

250. Plaintiff Voron stores any documents containing her Private Information in a safe and secure location. Plaintiff Voron has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

251. Because of the Data Breach, Plaintiff Voron's Private Information is now in the hands of cybercriminals.

252. Plaintiff Voron has suffered actual injury from the exposure and theft of her Private Information—which violates her right to privacy.

253. As a result of the Data Breach, which exposed highly valuable information such as her Social Security number, Plaintiff Voron is now imminently at risk of crippling future identity theft and fraud for her lifetime.

254. Plaintiff Voron has already begun to see the effects of Defendant's failures. During the relevant time, Plaintiff experienced suspicious activity of her bank account, which was determined to be fraudulent activity requiring Plaintiff Voron's time to set straight, including by working with her bank to be reimbursed for the charge, obtaining a new payment card, reviewing additional transactions, and changing many bill pay sites to reflect the new card.

255. Additionally, the loss of the use of her card for days leading up to the holiday season was a significant inconvenience for Plaintiff Voron, as it interrupted her ability to use her account.

256. This is only one example of the monetary loss of time that Plaintiff has and will continue to suffer as she faces the substantial increase in identity theft and fraud that Defendant's choices to forego reasonable cybersecurity investments has caused her.

257. Indeed, Plaintiff Voron has also received notifications that her Private Information has been located on the dark web following the Data Breach.

258. To help protect herself against the risk of identity theft and fraud, however, Plaintiff has invested in credit monitoring and identity theft protection services, which costs her just under $30 per month.

259. Further, as a result of the Data Breach, Plaintiff Voron has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Voron has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate and mitigate the future consequences of the Data Breach, including researching facts about the Data Breach, reviewing account statements and other information, monitoring her transactions and account activity on a regular basis, and taking other protective and ameliorative steps in response to the Data Breach. This is time that was lost and unproductive and took away from other activities, work, and family time.

260. The letter Plaintiff Voron received from Defendant specifically directed her to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised them to "remain vigilant by reviewing account statements and monitoring credit reports."[52] In addition, the breach notification letter listed several "recommended steps" that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, reviewing credit reports, placing fraud alerts with credit reporting bureaus, and placing security freezes on credit reports.[53]

261. As a result of the Data Breach, Plaintiff Voron has experienced stress, anxiety, fear and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing

[52] *Id.*
[53] *Id.*

and misusing her Private Information. Plaintiff Voron fears that criminals will use her information to commit identity theft.

262. Plaintiff Voron has spent and anticipates continuing to spend considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

263. Plaintiff Voron has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Voron's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Voron's Private Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Voron's Private Information; and (e) continued risk to Plaintiff Voron's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

PLAINTIFFS' AND CLASS MEMBERS' HARMS AND DAMAGES

264. To date, Defendant has done little to adequately protect Plaintiffs and Class Members, or to compensate them for their injuries sustained in this data breach. Defendant's Notice Letter downplays and disavows the theft of Plaintiffs' and Class Members' Private Information, when the facts demonstrate that the Private Information was accessed and exfiltrated. The complimentary fraud and identity monitoring service offered by Defendant is wholly inadequate as the services are only offered for one bureau and 12 months of coverage. The burden

is placed squarely on Plaintiffs and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this cybercrime.

265. Plaintiffs and Class Members have been injured and damaged by the compromise of their Private Information in the Data Breach.

266. Plaintiffs' and Class Members' Private Information (including but not limited to names, Social Security numbers, and PHI) was compromised in the Data Breach and is now in the hands of the cybercriminals who accessed Defendant's network.

267. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, tax return fraud, utility bills opened in their names, and similar identity theft.

268. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to target such schemes more effectively to Plaintiffs and Class Members.

269. Plaintiffs and Class Members will also incur out-of-pocket costs for protective measures such as credit monitoring fees (for any credit monitoring obtained in addition to or in lieu of the inadequate monitoring offered by Defendant), credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

270. Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was acquired by the hacker and cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

271. Plaintiffs and Class Members spent and will continue to spend significant amounts of time monitoring their financial accounts and records for misuse. Indeed, Defendant's own notice

of data breach provides instructions to Plaintiffs and Class Members about the significant time that they will need to spend monitoring their own accounts and statements received.

272. Plaintiffs spent many hours over the course of several days attempting to verify the veracity of the notice of breach and to monitor financial and online accounts for evidence of fraudulent activities.

273. Plaintiffs and Class Members suffered actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent loans, insurance claims, tax returns, and/or government benefit claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with credit reporting agencies;

d. Spending time on the phone with or at a financial institution or government agency to dispute fraudulent charges and/or claims;

e. Contacting financial institutions and closing or modifying financial accounts;

f. Closely reviewing and monitoring Social Security Number, bank accounts, and credit reports for unauthorized activity for years to come.

274. Defendant's delay in identifying and reporting the Data Breach caused additional harm. In a data breach, time is of the essence to reduce the imminent misuse of Private Information. Early notification helps a victim of a Data Breach mitigate their injuries, and conversely, delayed notification causes more harm and increases the risk of identity theft. Here, the breach occurred in September 2024, Defendant knew of it since October 6, 2024, and yet Defendant did not begin to notify the victims until December 12, 2024. Defendant offered no explanation or purpose for the delay.

275. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing sensitive and confidential personal, health, and/or financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

276. Further, as a result of Defendant's conduct, Plaintiffs and Class Members are forced to live with the anxiety that their Private Information may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

277. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class Members suffered a loss of privacy and are at a present, imminent, and increased risk of future harm.

CLASS ALLEGATIONS

278. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

279. The Classes that Plaintiffs seek to represent is defined as follows:

> All individuals in the United States whose Private Information was actually or potentially accessed or acquired during Defendant's Data Breach, including those to which Defendant sent Notice beginning on or around December 2024 ("Nationwide Class" or "Class").
>
> All individuals in the State of Illinois whose Private Information was actually or potentially accessed or acquired during Defendant's Data Breach, including those to which Defendant sent Notice beginning on or around December 2024 ("Illinois Subclass").

280. Excluded from the Classes are Defendant's officers and directors; any entity in

which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Classes are members of the judiciary to whom this case is assigned, their families and members of their staff.

281. Numerosity, Fed R. Civ. P. 23(a)(1): The Classes are so numerous that joinder of all members is impracticable. Defendant has identified hundreds of thousands of individuals whose Private Information may have been improperly accessed in the Data Breach, and the Classes are apparently identifiable within Defendant's records. Defendant advised the Maine Attorney General that the Data Breach affected approximately 450,000 individuals.

282. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the hacking incident and Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations, *e.g.*, FTC Guidelines, HIPAA, etc.;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Plaintiffs and Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Plaintiffs and Class Members to safeguard their Private Information;

g. Whether cybercriminals obtained Plaintiffs' and Class Members' Private Information in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Defendant owed a duty to provide Plaintiffs and Class Members timely notice of this Data Breach, and whether Defendant breached that duty to provide timely notice;

j. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

k. Whether Defendant's conduct was negligent;

l. Whether Defendant's conduct was *per se* negligent;

m. Whether Defendant breached any contractual duties to provide adequate security for the Private Information entrusted to it, duties that were either explicit or implied by the imposition of the membership fee.

n. Whether Defendant was unjustly enriched;

o. Whether Defendant's conduct violated federal laws;

p. Whether Defendant's conduct violated state laws; and

q. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, and/or punitive damages.

283. Common sources of evidence may also be used to demonstrate Defendant's unlawful conduct on a class-wide basis, including, but not limited to, documents and testimony about its data and cybersecurity measures (or lack thereof); testing and other methods that can prove Defendant's data and cybersecurity systems have been or remain inadequate; documents and testimony about the source, cause, and extent of the Data Breach; and documents and testimony about any remedial efforts undertaken as a result of the Data Breach.

284. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because all had their Private Information compromised as a result of the Data Breach and Defendant's misfeasance.

285. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that

is antagonistic or adverse to the Members of the Classes and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

286. Predominance, Fed. R. Civ. P. 23 (b)(3). Defendant engaged in a common course of conduct toward Plaintiffs and Class Members, in that all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

287. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

288. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would

necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Members to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

289. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

290. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

291. Unless a class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

292. Further, Defendant acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

293. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would

advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

e. Whether Defendant breached any contractual duty, either explicit or implied, to provide adequate data security as part of the membership fee;

f. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

g. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiffs and Class Members; and,

h. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

294. Defendant acted on grounds that apply generally to the Class as a whole, so that Class certification and the corresponding relief sought are appropriate on a Class-wide basis.

295. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CAUSES OF ACTION

FIRST COUNT
Negligence
(On Behalf of Plaintiffs and the Nationwide Class)

296. Plaintiffs repeat and re-allege each and every factual allegation contained in all

previous paragraphs as if fully set forth herein.

297. Plaintiffs bring this claim individually and on behalf of Class Members.

298. Plaintiffs and Class Members entrusted their Private Information to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their Private Information for purposes that would benefit Plaintiffs and Class Members and/or not disclose their Private Information to unauthorized third parties.

299. Defendant had full knowledge of the sensitive nature of the Private Information and the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information was wrongfully disclosed.

300. Defendant knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty included, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the Private Information of Plaintiffs and Class Members in Defendant's possession was adequately secured and protected.

301. Defendant had, and continues to have, a duty to timely disclose that Plaintiffs' and Class Members' Private Information within their possession was compromised and precisely the type(s) of information that were compromised.

302. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiffs' and Class Members' Private Information.

303. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards, applicable standards of care from statutory authority

like HIPAA and/or Section 5 of the FTC Act, and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

304. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Class Members, which is recognized by laws and regulations, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

305. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

306. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

307. Defendant systematically failed to provide adequate security for data in its possession.

308. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or Class Members.

309. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Upon information and belief, mishandling emails, so as to allow for unauthorized person(s) to access Plaintiffs' and Class Members' Private Information;

b. Failing to adopt, implement, and maintain adequate security measures to

safeguard Class Members' Private Information;

c. Failing to adequately monitor the security of their networks and systems;

d. Failure to periodically ensure that their computer systems and networks had plans in place to maintain reasonable data security safeguards.

310. Defendant, through its actions and/or omissions, unlawfully breached their duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information within Defendant's possession.

311. Defendant, through its actions and/or omissions, unlawfully breached their duty to Plaintiffs and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiffs' and Class Members' Private Information.

312. Defendant, through its actions and/or omissions, unlawfully breached their duty to timely disclose to Plaintiffs and Class Members that the Private Information within Defendant's possession might have been compromised and precisely the type of information compromised.

313. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiffs and Class Members' Private Information would result in injury to Plaintiffs and Class Members.

314. It was foreseeable that the failure to adequately safeguard Plaintiffs' and Class Members' Private Information would result in injuries to Plaintiffs and Class Members.

315. Defendant's breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' Private Information to be compromised.

316. As a result of Defendant's ongoing failure to notify Plaintiffs and Class Members regarding what type of Private Information has been compromised, Plaintiffs and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

317. Defendant's breaches of duties caused Plaintiffs and Class Members to suffer from

identity theft, loss of time and money to monitor their finances for fraud, and loss of control over their Private Information.

318. As a result of Defendant's negligence and breaches of duties, Plaintiffs and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

SECOND COUNT
Breach of Implied Contract
(On Behalf of Plaintiffs and the Nationwide Class)

319. Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

320. Defendant, as a condition of providing its services, required Plaintiffs' and Class Members to provide and entrust their Private Information.

321. By Plaintiffs and Class Members providing their Private Information, and by Defendant accepting this Private Information and representing it would maintain the safety and security of this Private information, including through its privacy policies, the parties mutually assented to implied contracts. These implied contracts included an implicit agreement and understanding that (1) Defendant would adequately safeguard Plaintiffs' and Class Members' Private Information from foreseeable threats, (2) that Defendant would delete the information of Plaintiffs and Class Members once it no longer had a legitimate need; and (3) that Defendant would provide Plaintiffs and Class Members with notice within a reasonable amount of time after suffering a data breach.

322. Defendant provided consideration by providing it services, while Plaintiffs and Class Members provided consideration by paying for its services and providing valuable property—*i.e.*, their Private Information and payment to Defendant. Defendant benefitted from the

receipt of this Private Information by increased income through providing medical services.

323. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

324. Defendant breached its implied contracts with Plaintiffs and Class Members by failing to safeguard and protect their Private Information or providing timely and accurate notice to them that their Private Information was compromised due to the Data Breach.

325. Defendant's breaches of contract have caused Plaintiffs and Class Members to suffer damages from the lost benefit of their bargain, out-of-pocket monetary losses and expenses, loss of time, and diminution of the value of their Private Information.

326. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and Class Members have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

THIRD COUNT
Unjust Enrichment
(On Behalf of Plaintiffs and the Nationwide Class)

327. Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

328. Plaintiffs plead this Count in the alternative to their Implied Contract claim.

329. Plaintiffs and Class Members conferred a monetary benefit on Defendant, by providing Defendant with their valuable Private Information in exchange for medical treatment.

330. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information.

331. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

332. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

333. Defendant acquired the monetary benefit and Private Information through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

334. If Plaintiffs and Class Members knew that Defendant had not secured their Private Information, they would not have agreed to provide it to Defendant.

335. Plaintiffs and Class Members have no adequate remedy at law.

336. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control or direct how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses

associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in its continued possession and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

337. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

338. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them.

FOURTH COUNT
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Nationwide Class)

339. Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

340. In light of the special relationship between Defendant and Plaintiffs and Class Members, whereby Defendant became guardian of Plaintiffs' and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiffs and Class Members, (1) for the safeguarding of

Plaintiffs' and Class Members' Private Information; (2) to timely notify Plaintiffs and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

341. Further, Defendant had a fiduciary duty as a healthcare provider to maintain the confidentiality its patients' private information shared with it in the course of treatment, including Plaintiffs and Class Members' Private Information.

342. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its relationship with its current and former patients and employees to keep secure their Private Information. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently discover, investigate, and give detailed notice of the Data Breach to Plaintiffs and Class in a reasonable and practicable period of time.

343. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiffs' and Class Members' Private Information.

344. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach.

345. Defendant breached its fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Private Information.

346. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated

with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (vii) the diminished value of Defendant's services they received.

347. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

FIFTH COUNT
Invasion of Privacy
(On Behalf of Plaintiffs and the Nationwide Class)

348. Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

349. Plaintiffs and Class Members had a reasonable expectation of privacy in the Private Information Defendant mishandled.

350. As a result of Defendant's conduct, publicity was given to Plaintiffs' and Class Members' Private Information, which necessarily includes matters concerning their private life such as PII and PHI.

351. A reasonable person of ordinary sensibilities would consider the publication of Plaintiffs' and Class Members' Private Information to be highly offensive.

352. Plaintiffs' and Class Members' Private Information is not of legitimate public concern and should remain private.

353. As a direct and proximate result of Defendant's public disclosure of private facts, Plaintiffs and Class Members are at a current and ongoing risk of identity theft and sustained compensatory damages including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution of value of their Private Information; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their Private Information, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

354. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

355. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

SIXTH COUNT
Declaratory and Injunctive Relief
(On Behalf of Plaintiffs and the Nationwide Class)

356. Plaintiffs repeat and re-allege each and every factual allegation contained in all

previous paragraphs as if fully set forth herein.

357. Plaintiffs pursue this claim under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

358. Defendant owed a duty of care to Plaintiffs and Class Members that require it to adequately secure Plaintiffs' and Class Members' Private Information.

359. Defendant failed to fulfill their duty of care to safeguard Plaintiffs' and Class Members' Private Information.

360. As described above, actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiffs and Class Members. Further, Plaintiffs and Class Members are at risk of additional or further harm due to the exposure of their Private Information and Defendant's failure to address the security failings that led to such exposure.

361. There is no reason to believe that Defendant's employee training and security measures are any more adequate now than they were before the breach to meet Defendant's contractual obligations and legal duties.

362. Plaintiffs, therefore, seeks a declaration (1) that Defendant's existing data security measures do not comply with their contractual obligations and duties of care to provide adequate data security, and (2) that to comply with their contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to, the following:

SEVENTH COUNT
Violation of the Illinois Consumer Fraud Act
815 Ill. Comp. Stat. §§ 505/1, *et seq.*
(On Behalf of Plaintiff Kelley and the Illinois Subclass)

363. Plaintiff Kelley ("Plaintiff" for the purposes of this count) repeats and re-alleges

each and every factual allegation contained in all previous paragraphs as if fully set forth herein and brings this claim on behalf of herself and the Illinois Subclass (the "Class" for the purposes of this count).

364. Plaintiff and Class Members are "consumers" as that term is defined in 815 Ill. Comp. Stat. § 505/1(e).

365. Plaintiff, Class Members, and Defendant are "persons" as that term is defined in 815 Ill. Comp. Stat. § 505/1(c).

366. Defendant is engaged in "trade" or "commerce," including the provision of services, as those terms are defined under 815 Ill. Comp. Stat. § 505/1(f).

367. Defendant engages in the "sale" of "merchandise" (including services) as defined by 815 Ill. Comp. Stat. § 505/1(b) and (d).

368. Defendant's acts, practices, and omissions were done in the course of Defendant's business of marketing, offering for sale, and selling medical services in the State of Illinois.

369. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts in connection with the sale and advertisement of "merchandise" (as defined in the Illinois Consumer Fraud Act ("CFA")) in violation of the Illinois CFA, including, but not limited to, the following:

a. failure to maintain adequate computer systems and data security practices to safeguard current and former patients' Private Information;

b. failure to disclose the material fact that its computer systems and data security practices were inadequate to safeguard the Private Information it was collecting and maintaining from theft;

c. failure to disclose in a timely and accurate manner to Plaintiff and Class

Members the material fact of Defendant's data breach;

d. misrepresenting material facts to Plaintiff and Class Members, in connection with the sale of goods and services, by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff's and Class Members' Private Information from unauthorized disclosure, release, data breaches, and theft;

e. misrepresenting material facts to the class, in connection with the sale of goods and services, by representing that Defendant did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff's and Class Members' Private Information, and

f. failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff's and Class Members' Private Information from further unauthorized disclosure, release, data breaches, and theft.

370. In addition, Defendant's failure to disclose that its computer systems were not well protected and that Plaintiff's and Class Members' sensitive information was vulnerable and susceptible to intrusion and cyberattacks constitutes deceptive and/or unfair acts or practices because Defendant knew such facts would (a) be unknown to and not easily discoverable by Plaintiff and Class Members; and (b) defeat Plaintiff's and Class Members' ordinary, foreseeable and reasonable expectations concerning the security of their Private Information on Defendant's servers.

371. Defendant intended that Plaintiff and Class Members rely on its deceptive and unfair acts and practices, misrepresentations, and the concealment, suppression, and omission of

material facts, in connection with Defendant's offering of goods and services and storing Plaintiff's and Class Members' Private Information on its servers, in violation of the Illinois CFA.

372. Defendant also engaged in unfair acts and practices by failing to maintain the privacy and security of class members' Private Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach.

373. These unfair acts and practices violated duties imposed by laws including Section 5 of the Federal Trade Commission Act (15 U.S.C. § 45), HIPAA, and similar state laws.

374. Defendant's wrongful practices occurred in the course of trade or commerce.

375. Defendant's wrongful practices were and are injurious to the public interest because those practices were part of a generalized course of conduct on the part of Defendant that applied to all Class Members and were repeated continuously before and after Defendant obtained Private Information from Plaintiff and Class Members.

376. All Class Members have been adversely affected by Defendant conduct and the public was and is at risk as a result thereof.

377. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered harm, as alleged herein.

378. Pursuant to 815 Ill. Comp. Stat. § 505/10a(a), Plaintiff seeks actual, compensatory, and punitive damages (pursuant to 815 Ill. Comp. Stat. § 505/10a(c)), injunctive relief, and court costs and attorneys' fees as a result of Defendant's violations of the Illinois CFA.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, pray for relief as follows:

A. For an Order certifying this case as a class action and appointing Plaintiffs and

Plaintiffs' counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

E. Ordering Defendant to pay for not less than three years of credit monitoring services for Plaintiffs and the Class;

F. Ordering Defendant to disseminate individualized notice of the Data Breach to all Class Members;

G. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

H. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

I. Pre- and post-judgment interest on any amounts awarded; and

J. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury of all claims so triable.

Dated: February 21, 2025

Respectfully submitted,

/s/ Donald J. Enright

Donald J. Enright (#13551)
Jordan A. Cafritz (#20908)
LEVI & KORSINSKY, LLP 1101
Vermont Ave. NW, Suite 700
Washington, D.C. 20005
Tel: (202) 524-4290
Email: denright@zlk.com
Email: jcafritz@zlk.com

Interim Liaison Counsel for Plaintiffs

Jeff Ostrow
KOPELOWITZ OSTROW P.A.
1 W. Las Olas Blvd., Ste. 500
Fort Lauderdale, FL 33301
Telephone: (954) 525-4100
ostrow@kolawyers.com

David K. Lietz *
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Ave., NW, Suite 440
Washington, DC 20015
Phone: 866.252.0878
dlietz@milberg.com

A. Brooke Murphy *
MURPHY LAW FIRM
4116 Will Rogers Pkwy, Suite 700
Oklahoma City, OK 73108
Telephone: (405) 389-4989
abm@murphylegalfirm.com

Andrew J. Shamis, Esq.
SHAMIS & GENTILE P.A.
TX Bar No. 24124558
ashamis@shamisgentile.com
14 NE 1st Ave., Suite 705
Miami, Florida 33132
Telephone: 305-479-2299

Interim Class Counsel for Plaintiffs

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that a true and correct copy of the foregoing has been served upon all counsel of record for each party in the consolidated action via electronic mail on this February 21, 2025.

/s/ Donald J. Enright
Donald J. Enright